EV257330061US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Keith Alexander HARRISON, et al.	RE: Claim to Priority
Serial No.: Not yet assigned	
Filed: Concurrently herewith	Our Ref: B-5172 621109-9
For: "METHOD AND APPARATUS FOR SECURELY TRANSFERRING DATA"	Date: July 17, 2003

CLAIM TO PRIORITY UNDER 35 U.S.C. 119

Mail Stop Patent Application
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450
Sir:

[X] Applicants hereby make a right of priority claim under 35 U.S.C. 119 for the benefit of the filing date(s) of the following corresponding foreign application(s):

COUNTRY	FILING DATE	SERIAL NUMBER
GB	18 July 2002	0216690.8

[ ] A certified copy of each of the above-noted patent applications was filed with the Parent Application No.__.

[X] To support applicants' claim, a certified copy of the above-identified foreign patent application is enclosed herewith.

[ ] The priority document will be forwarded to the Patent Office when required or prior to issuance.

Respectfully submitted,

Ross A. Schmitt
Attorney for Applicant
Reg. No. 42,529

LADAS & PARRY
5670 Wilshire Boulevard
Suite 2100
Los Angeles, CA 90036
Telephone: (323) 934-2300
Telefax: (323) 934-0202

The Patent Office
Concept House
Cardiff Road
Newport
South Wales
NP10 8QQ

I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

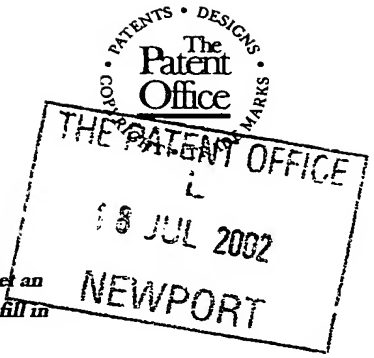
Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.

Signed

Dated 13 September 2002

Patents Form 1/77

Paten[illegible] Act 1977
(Rul[illegible])



18JUL02 E734256-1 001463
P01/7700 0.00-0216690.8

Request for grant of a patent

(See the notes on the back of this form. You can also get an explanatory leaflet from the Patent Office to help you fill in this form)

The Patent Office

Cardiff Road
Newport
South Wales
NP10 8QQ

1. Your reference — 300110457-01 GB

2. Patent application number
(The Patent Office will fill in this part) — 0216690.8

3. Full name, address and postcode of the or of each applicant *(underline all surnames)*

Hewlett-Packard Company
3000 Hanover Street
Palo Alto
CA 94304, USA

Patents ADP number *(if you know it)* 4965880004

If the applicant is a corporate body, give the country/state of its incorporation — Delaware, USA

4. Title of the invention — Method and apparatus for encrypting data

5. Name of your agent *(if you have one)*

"Address for service" in the United Kingdom to which all correspondence should be sent *(including the postcode)*

Chris Harrison
Hewlett-Packard Ltd, IP Section
Filton Road, Stoke Gifford
Bristol BS34 8QZ

Patents ADP number *(if you know it)* 8191439001

6. If you are declaring priority from one or more earlier patent applications, give the country and the date of filing of the or of each of these earlier applications and *(if you know it)* the or each application number

Country	Priority application number *(if you know it)*	Date of filing *(day / month / year)*

7. If this application is divided or otherwise derived from an earlier UK application, give the number and the filing date of the earlier application

Number of earlier application	Date of filing *(day / month / year)*

8. Is a statement of inventorship and of right to grant of a patent required in support of this request? *(Answer 'Yes' if:*

a) any applicant named in part 3 is not an inventor, or
b) there is an inventor who is not named as an applicant, or
c) any named applicant is a corporate body.
See note (d))

Yes

Patents Form 1/77

9. Enter the number of sheets for any of the following items you are filing with this form. Do not count copies of the same document

Continuation sheets of this form	
Description	10
Claim(s)	2
Abstract	1 DMC
Drawing(s)	2+2

10. If you are also filing any of the following, state how many against each item.

Priority documents	
Translations of priority documents	
Statement of inventorship and right to grant of a patent *(Patents Form 7/77)*	1
Request for preliminary examination and search *(Patents Form 9/77)*	1
Request for substantive examination *(Patents Form 10/77)*	
Any other documents *(please specify)*	Fee Sheet

11. I/We request the grant of a patent on the basis of this application.

Signature [signature] Date 17/7/2002

12. Name and daytime telephone number of person to contact in the United Kingdom — Tony Judd — Tel: 0117-312-8026

Warning

After an application for a patent has been filed, the Comptroller of the Patent Office will consider whether publication or communication of the invention should be prohibited or restricted under Section 22 of the Patents Act 1977. You will be informed if it is necessary to prohibit or restrict your invention in this way. Furthermore, if you live in the United Kingdom, Section 23 of the Patents Act 1977 stops you from applying for a patent abroad without first getting written permission from the Patent Office unless an application has been filed at least 6 weeks beforehand in the United Kingdom for a patent for the same invention and either no direction prohibiting publication or communication has been given, or any such direction has been revoked.

Notes

a) *If you need help to fill in this form or you have any questions, please contact the Patent Office on 08459 500505.*

b) *Write your answers in capital letters using black ink or you may type them.*

c) *If there is not enough space for all the relevant details on any part of this form, please continue on a separate sheet of paper and write "see continuation sheet" in the relevant part(s). Any continuation sheet should be attached to this form.*

d) *If you have answered 'Yes' Patents Form 7/77 will need to be filed.*

e) *Once you have filled in the form you must remember to sign and date it.*

f) *For details of the fee and ways to pay please contact the Patent Office.*

METHOD AND APPARATUS FOR ENCRYPTING DATA

The present invention relates to a method and system for encrypting data.

With the wide spread use of the Internet commercial transactions over the Internet have become commonplace. However, unlike commercial transactions that are conducted face-to-face, transactions over the Internet typically involve the exchange of private and confidential information, for example providing access to a party's bank account details, credit card details and home address.

Accordingly, many individuals still have concerns over confidentiality; as a result the full potential of the Internet is still not being utilized.

It is desirable to improve this situation.

In accordance with a first aspect of the present invention there is provided a computer system comprising a first computer entity arranged to encrypt a first data set with a first encryption key associated with a third party to generate a third data set and encrypt a fourth data set with the third data set; communication means for providing the encrypted fourth data set to a second computer entity and the third data set to a third computer entity associated with the third party; wherein the third computer entity is arranged to generate a decryption key using the third data set to allow the second computer entity to decrypt the encrypted fourth data set.

This provides the advantage of restricting access to information associated with a transaction between a first and second party such that the parties to the transaction only have access to information relevant to them. For example, for

a transaction between a first and second party the second party may only need to know that they will be paid, accordingly credit card or bank account details can be encrypted and forward to the first party's bank who, on decrypting the information, can then credit the second party's account, thereby ensuring that the second party does not have access to the first party's bank account or credit card details.

Preferably the first encryption key corresponds to a public key associated with the third party.

Preferably the third computer entity is arranged to decrypt the third data set with the third party's corresponding private key.

Preferably the first data set corresponds to a message for the third party.

Preferably the third computer entity is arranged to provide the decryption key to the second computer entity.

In accordance with a second aspect of the present invention there is provided a computer apparatus comprising a processor arranged to encrypt a first data set with a first encryption key associated with a third party to generate a third data set and encrypt a fourth data set with the third data set.

Preferably the computer apparatus further comprises means for providing the encrypted fourth data set to a second computer entity.

In accordance with a third aspect of the present invention there is provided a method for encrypting data comprising encrypting a first data set with a first encryption key associated with a third party to generate a third data set and encrypting a fourth data set with the third data set.

For a better understanding of the present invention and to understand how the same may be brought into effect reference will now be made, by way of example only, to the accompanying drawings, in which:-

Figure 1 illustrates a computer system according to an embodiment of the present invention;

Figure 2 illustrates the generation of encrypted data according to an embodiment of the present invention.

The present embodiment describes a computer system that allows a user to place an electronic order with a service provider where the service provider has restricted access to the user's private and confidential information necessary to complete the order.

In particular, the user is able to place an electronic order with the service provider, where confidential information required by the service provider to complete the transaction, for example the user's address, is encrypted with an encryption key, where the encryption key is in itself an encrypted message from the user to the user's bank. The bank, acting as a trusted authority, is the only entity that is able to derive the associated decryption key. Accordingly, for the service provider to complete the transaction the service provider must provide the encryption key to the bank to allow the bank to derive the associated decryption key. On receipt of the encryption key the bank decrypts the encryption key to access the message, that can, for example, include instructions to pay the service provider, while also providing the associated decryption key to the service provider to allow them to decrypt the encrypted confidential information provided by the user to the service provider.

Figure 1 illustrates a computer system 10 according to an embodiment of the present invention. Computer system 10 includes a first computer entity 11, a

second computer entity 12 and a third computer entity 13. Typically the three computer entities 11, 12, 13 would be configured on separate computer platforms, however the computer entities 11, 12, 13 could be configured on a single computer platform. For the purposes of this embodiment, however, the three computer entities 11, 12, 13 are coupled via a network 14, for example the Internet.

Associated with the second computer entity 12 is a service provider 18 that offers goods and/or services over the service provider's website (not shown) accessible via the network 14, however, as would be appreciated by a person skilled in the art the service provider 18 could offer goods and/or services via a variety of ways, for example via email.

The first computer entity 11 is configured to allow a user 19 to access the service provider 18, via the second computer entity 12, to allow the user 19 to place an order with the service provider 18 for goods and/or service, as described below.

Associated with the third computer entity 13 is a bank 15 with which the user 19 has a bank and credit card account. The bank 15 is configured to act as a trust authority 16. Additionally, the bank 15, acting as a trust authority 16, makes publicly available the trust authorities public data 17, as described below. As would be appreciated by a person skilled in the art the trust authorities public data 17 can be made available in a variety of ways, for example via a public web site (not shown).

Using the first computer entity 11 the user 19 completes an order form for ordering specific goods and/or services from the service provider 18 where information within the order form may have different categorisations, for example part of the order may be deemed non-confidential such as goods and/or services required and associated quantities, while other parts of the

order may be deemed to be confidential, such as the user's address required for delivery. However, payment details are not included within the order

In addition, however, the user 19 also generates a payment message for the attention of the user's bank 15 that contains payment information relevant to the user's order with the service provider 18, for example the user's bank account number and the amount to be paid to the service provider 18.

Using the first computer entity 11 the user 19 generates an encryption key to encrypt the order form for goods and/or services required from the service provider 19 where the encryption key is derived by encrypting the payment message with a public key associated with the bank 15 from which the user 19 derives a representative digital string of data bits (i.e. the public key string) where this string acts as the user's encryption key. As such, the encryption key is derived using an identifier based encryption IBE scheme, where the following description is based upon a QR based IBE scheme, however, other IBE schemes could be used, for example schemes based upon Tate and Weil pairings.

The bank's public key used to encrypt the payment message can be obtained by any suitable means, for example the public key could be PKI based or identity based encryption IBE based.

Once the encryption key has been derived the confidential information can be encrypted with the encryption key, as described below, thereby allowing the user 19 to forward to the service provider 18 an encrypted order form. Where the information within the order form has been categorised as either confidential or non-confidential only the confidential information need be encrypted, in this situation the order form would consist of a combination of plaintext and encrypted text.

To allow the user 19, using the first computer entity 11, to generate an encryption key and encrypt the order form the user may use a software plug-in 20.

The software plug-in 20 may, for example, be obtained from the trust authority's web site (not shown) where the plug-in 20 can be installed within the user's web browser (not shown). The plug-in 20 embeds knowledge regarding the trust authorities public details N, # 17, as described below.

The plug-in 20 is arranged to encrypt the order form information classified as confidential, where each bit of the information is defined by M, as described below.

The trust authorities public data 17 includes a hash function # and a value N that is a product of two random prime numbers p and q, where the values of p and q are only known to the trust authority.

The hash function # has the function of taking a string and returning a value in the range 0 to N. Additionally, the hash function # should have the jacobi characteristics: jacobi (#, N) = 1. That is to say, where $x^2 \equiv \# \bmod N$ the jacobi (#, N) = -1 if x does not exist, and = 1 if x does exist.

The values of p and q should ideally be in the range of 2^{511} and 2^{512} and should both satisfy the equation: $p,q \equiv 3 \bmod 4$. However, p and q must not have the same value.

To encrypt each bit M of the order form the user 19 generates random numbers t_+ (where t_+ is an integer in the range [0, 2^N)) until the user 19 finds a value of t_+ that satisfies the equation $jacobi(t_+, N) = M$, where M represents the individual binary digits 0, 1 of the user's data as –1, 1 respectively. The user 19 then computes the value:

$$s_+ = (t_+ + \#(publickeystring)/t_+) \bmod N .$$

for each bit M where s_+ corresponds to the encrypted bit of M.

In case #(publickeystring) is non-square the user 19 additionally generates additional random numbers t_- (integers in the range [0, 2^N)) until the user 19 finds one that satisfies the equation $jacobi(t_-, N) = m$. The user 19 then computes the value:

$$s_- = (t_- - \#(publickeystring)/t_-) \bmod N$$

for each value of bit M.

The non-encrypted and encrypted order form information and encryption key is made available to the service provider 18 by any suitable means, for example via e-mail or by being placed in a electronic public area.

For the service provider 18 to recover the associated decryption key the service provider 18 provides the encryption key, as used by the user 19 to encrypt the order form, to the trust authority 16.

The trust authority 16 determines the associated decryption key B by solving the equation :

$$B^2 \equiv \#(publickeystring) \bmod N$$

If a value of B does not exist, then there is a value of B that is satisfied by the equation:

$$B^2 \equiv -\#(publickeystring) \bmod N$$

As N is a product of two prime numbers p, q it would be extremely difficult for any one to calculate the private key B with only knowledge of the public key string and N. However, as the trust authority 16 has knowledge of p and q (i.e. two prime numbers) it is relatively straightforward for the trust authority 16 to calculate B.

Any change to the encryption key will result in a decryption key that will not decrypt the order form correctly, thereby preventing the service provider from understanding the order.

If the square root of the encryption key returns a positive value, the user's data M can be recovered using:

$$M = jacobi(s_+ + 2B, N).$$

If the square root of the encryption key returns a negative value, the user's data M can be recovered using:

$$M = jacobi(s_- + 2B, N).$$

The service provider 18 uses the appropriate equation above, in conjunction with the encryption key, to decrypt the message and on receipt of payment from the trust authority, as described below, the service provider provides the requested goods and/or services to the user 19.

Additionally, the trust authority decrypts the encryption key using the appropriate trust authorities private key, thereby allowing the trust authority to read the payment message created by the user 19.

Accordingly, in accordance with the user's instructions contained within the payment message the trust authority 16 initiates payment to the service provider 18 for payment of the goods and/or services ordered by the user 19 without the service provider 18 requiring any access to the user's payment details.

Further, the encryption key derived from the encrypted payment message could be made dependent on dynamic information, for example time and/or a random number.

Additionally, the communication between the various parties can make use of standard protocols such as HTTP and SOAP. Further, where required secure connections can be established using secure protocols such as SSL.

Figure 2 illustrates the stages of encryption of data associated with a transaction between the user 19 and the service provider 18.

The trust authority 16 publishes its public details N, # 17.

The first computer entity 11, using a public key 20 associated with the trust authority 16, encrypts a payment message 21 intended for the trust authority 16 to generate an encryption key 22. The first computer entity 11 then, using the encryption key 22, encrypts an order form 23 intended for the service provider 18 to generate encrypted data 24.

The encryption key 22 is provided to the third computer entity 13 to allow the trust authority 16 to decrypt the payment message 21and derive an associated decryption key 25 for the encrypted data 24.

The encrypted data 24 is provided by the first computer entity 11 to the second computer entity 12 with the third computer entity 13 providing the

associated decryption key 25 to the second computer entity 12, thereby allowing the service provider 18 to decrypt the order form 23.

CLAIMS

1. A computer system comprising a first computer entity arranged to encrypt a first data set with a first encryption key associated with a third party to generate a third data set and encrypt a fourth data set with the third data set; communication means for providing the encrypted fourth data set to a second computer entity and the third data set to a third computer entity associated with the third party; wherein the third computer entity is arranged to generate a decryption key using the third data set to allow the second computer entity to decrypt the encrypted fourth data set.

2. A computer system according to claim 1, wherein the first encryption key corresponds to a public key associated with the third party.

3. A computer system according to claim 1 or 2, wherein the third computer entity is arranged to decrypt the third data set with the third party's corresponding private key.

4. A computer system according to any preceding claim, wherein the first data set corresponds to a message for the third party.

5. A computer system according to any preceding claim, wherein the third computer entity is arranged to provide the decryption key to the second computer entity.

6. A computer apparatus comprising a processor arranged to encrypt a first data set with a first encryption key associated with a third party to generate a third data set and encrypt a fourth data set with the third data set.

7. A computer apparatus according to claim 6, further comprising means for providing the encrypted fourth data set to a second computer entity.

8. A computer apparatus according to claim 6 or 7, wherein the first data set corresponds to a message for the third party.

9. A computer apparatus according to any of claims 6 to 8, wherein the first encryption key corresponds to a public key associated with the third party.

10. A method for encrypting data comprising encrypting a first data set with a first encryption key associated with a third party to generate a third data set and encrypting a fourth data set with the third data set.

11. A method according to claim 10, further comprising providing the fourth data set to a second party.

12. A method according to claim 11, further comprising providing the third data set to the third party to allow the generation of a decryption key using the third data set to allow the second party to decrypt the encrypted fourth data set.

13. A method according to claim 12, further comprising providing to the second party from the third party the decryption key.

ABSTRACT

METHOD AND APPARATUS FOR ENCRYPTING DATA

A computer system comprising a first computer entity arranged to encrypt a first data set with a first encryption key associated with a third party to generate a third data set and encrypt a fourth data set with the third data set; communication means for providing the encrypted fourth data set to a second computer entity and the third data set to a third computer entity associated with the third party; wherein the third computer entity is arranged to generate a decryption key using the third data set to allow the second computer entity to decrypt the encrypted fourth data set.

Figure 1

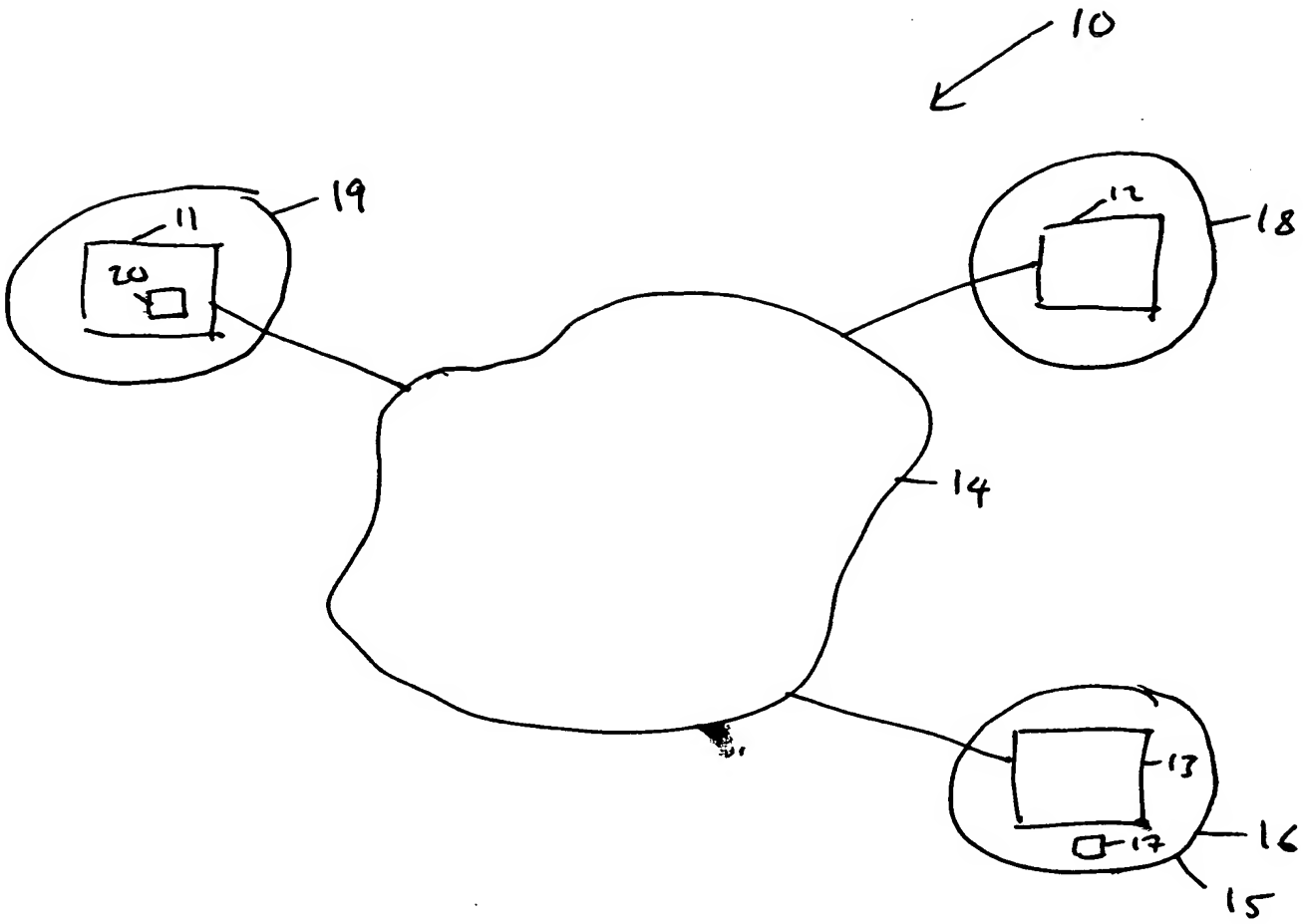


Figure 1

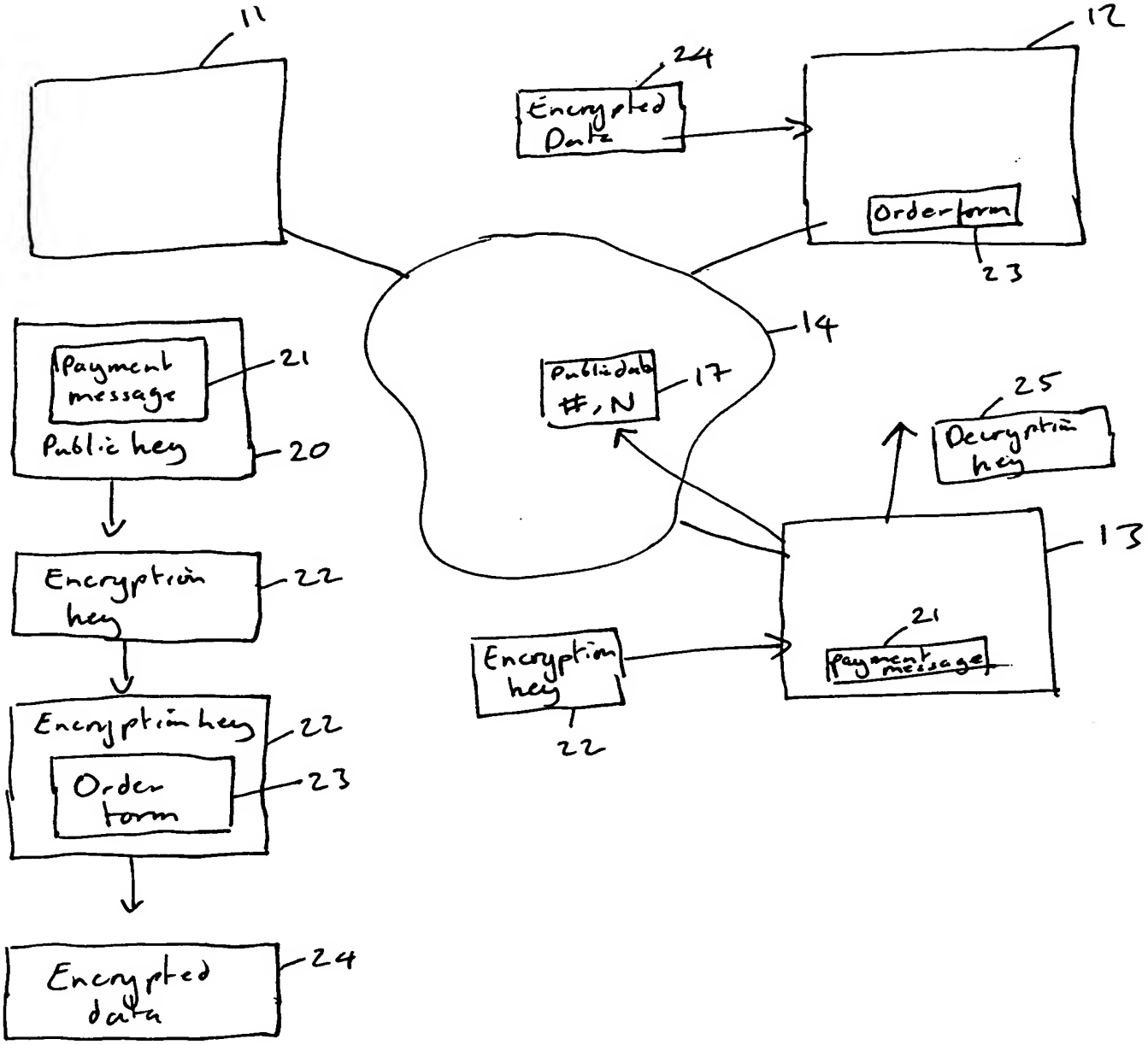

11
12
24
Encrypted Data
Order form
23
14
Payment message
21
Public key
20
Public data #, N
17
25
Decryption key
Encryption key
22
13
Encryption key
22
21
Payment message
Encryption key
22
Order form
23
Encrypted data
24

Figure 2